Publication No. : 000036707 (20000705)

Application No. : 000015429 (20000327)

Title of Invention : METHOD FOR VERIFYING HOME PAGE BY ELECTRON IC AUTHENTICATION

Document Code : A

IPC : G06F 17/00

Priority :

Applicant : DREAM SECURITY CO., LTD.

Inventor : KIM, DAE SIK

Abstract :

PURPOSE: A method for verifying home page by an electronic authentication is provided so that a reliable internet environment can be constructed and a cyber-crime can be prevented by understanding whether document of static or dynamic produced on the web is true or false according to the request of the web browser and notifying it.

CONSTITUTION: A method for verifying home page by electronic authentication includes several steps. When transmitting documents of static or dynamic, at the state that the static document electronically signed is produced through the cryptographic process previously by a web page authentication program and is stored to the directory, if in a home page, a user requests the authentication about the home page, a step is to transmit a dynamically signed document from a web server to a web page authentication server. The dynamic document produced by the web server application program is produced an electronic signed document by the cryptographic process at the web page authentication server and transmitted the static or dynamic document to the web browser. Thereafter, the web browser calls a web page authentication client and identifies the electronic sign of the static or dynamic document through the predetermined decoding process. If the sign is true, the static or dynamic is transmitted to the web browser.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
G06F 17/00

(11) 공개번호 특2000-0036707
(43) 공개일자 2000년07월05일

(21) 출원번호 10-2000-0015429
(22) 출원일자 2000년03월27일

(71) 출원인 주식회사 드림시큐리티 윤금
서울특별시 성북구 성북동 94-1 성북프라자 6층
(72) 발명자 김대식
서울특별시마포구염리동36-154
(74) 대리인 김영철

심사청구 : 있음

(54) 전자인증에 의한 홈 페이지 검증방법

요약

본 발명은 웹 서버에서 정적 문서와 동적 문서를 웹 브라우저에 전송시, 정적 문서는 사전에 웹 페이지 인증 프로그램으로 암호화 과정을 거쳐 전자 서명한 정적 서명된 문서를 생성하여 디렉토리에 저장시킨 상태에서 웹 브라우저에서 홈 페이지에 대한 인증 요청을 하면 웹 서버에서 웹 페이지 인증 서버로 정적 서명된 문서를 전송하고, 웹 서버 응용 프로그램에 의해 생성된 동적 문서는 웹 페이지 인증 서버에서 암호화 과정을 거쳐 전자 서명한 동적 서명된 문서를 생성하여 동적 또는 정적 서명된 문서를 웹 브라우저로 전송하고, 웹 브라우저로 정적 또는 동적 서명된 문서가 전송되면 웹 브라우저는 웹 페이지 인증 클라이언트를 호출하여 웹 페이지 인증 클라이언트에서 소정의 복호화 과정을 거쳐 전송된 정적 문서 또는 동적 문서의 전자 서명이 정당한지의 여부를 파악하여 서명이 정당하면 정적 문서 또는 동적 문서를 웹 브라우저로 전송하는 것을 특징으로 한다.

따라서 상기와 같이 이루어진 본 발명에 따르면 웹 브라우저의 요청에 따라 웹 페이지 인증 서버에서 생성되는 정적 또는 동적 문서의 진위 여부를 파악하여 사용자에게 알림으로써 신뢰할 수 있는 인터넷 환경을 구축할 수 있다.

대표도

도2a

색인어

홈 페이지 인증, 웹 브라우저, 웹 페이지 인증 서버

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 전자인증에 의한 홈 페이지 검증방법의 개념을 설명하기 위한 개념도

도 2a 내지 도 2c는 본 발명에 따른 전자인증에 의한 홈 페이지 검증방법을 설명하기 위한 동작 흐름도

〈도면중 주요부분에 대한 부호의 설명〉

100 : 웹 브라우저 200 : 웹 페이지 인증 클라이언트
300 : 웹 페이지 인증 서버 400 : 웹 서버
500 : 웹 페이지 인증 프로그램 600 : 웹 서버 응용 프로그램
700 : 웹 문서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 홈페이지 검증방법에 관한 것으로, 더욱 상세하게는 사용자, 즉 웹 브라우저에서 웹 서버에게 홈페이지의 인증을 요청하여 웹 서버를 통해 전송되는 홈페이지에 대해 웹 페이지 인증 서버와 웹 페이지 인증 프로그램과 웹 페이지 인증 클라이언트에서 인증을 수행하여 홈페이지의 진위 여부를 파악한 후

사용자에게 홈페이지의 진위 여부를 알리는 전자인증에 의한 홈페이지 검증 방법에 관한 것이다.

잘 알려진 바와 같이, 초기의 인터넷은 특수한 군사 목적의 컴퓨터 네트웍으로 출발하였으나, 현재에는 전세계의 모든 국가 또는 지역의 컴퓨터들을 연결하는 대중적인 네트웍으로 자리매김되어 있다. 이러한 인터넷의 기원은 1960년대 미국 국방성이 전략 방위적 목적으로 구축한 ARPAnet인데, 냉전 시대에 군사적인 목적으로 개발된 첨단 기술이 그 시대적 변화에 따라 정보화 시대가 도래하자 일반인의 생활에 큰 도움을 줄 수 있는 대중매체로 탈바꿈하게 된 것이다.

초기의 인터넷 목적은 학문 연구의 수단으로 이용되는 것이었으나, 그 발전과 동시에 인터넷의 이용 방향은 학술, 경제, 문화 등 사회 각 분야로 넓혀지기 시작했다.

인터넷은 그 발생에서부터 어떠한 상태에서도 서로 떨어져 있는 두 컴퓨터간의 통신을 원활하게 유지하기 위하여 고안된 네트웍이며, 인터넷의 모체인 ARPAnet은 패킷(packet) 통신을 기반으로 하여 구축되었으며, 1973년에는 ARPAnet이 영국과 노르웨이에 최초의 해외 접속을 개시하였으며, 1974년에 이르러 패킷 교환망 프로토콜인 TCP(Transmission Control Protocol)를 디자인하기에 이르렀다.

이후, 확장을 계속하던 ARPAnet은 1982년에 이르러 인터넷의 핵심 기술이라고 할 수 있는 TCP/IP(Transmission Control Protocol/Internet Protocol)를 이용해 구축함으로써 인터넷이 도입되기 시작하여 1984년에는 미국의 UUCP와 접속하여 전자 우편 서비스를 개시하였으며, 1988년 한국의 도메인이 (.kr)로 규정되기 시작하면서 각종 인터넷 서비스에 적용되기 시작하였다.

이와 같은 인터넷은 하이퍼텍스트를 기반으로 한 월드 와이드 웹 서비스가 개발되면서 급속한 발전을 가져왔다.

월드 와이드 웹(WWW : World Wide Web)은 1989년 유럽 입자 물리 연구소(The European Laboratory for Particle Physics, CERN)의 Tim Berners-Lee에 의하여 클라이언트/서버(Client/Server)모델을 기반으로 유럽 입자 물리 연구소에 산재되어 있는 문서의 효율적 정리와 검색을 위해 개발되었다.

그리고 하이퍼텍스트(hyper text)는 기존의 고퍼(gopher), 웨이스(WAIS)와 같은 메뉴 형식을 벗어나 지정된 자료와 직접 연결이 가능하게 하는 네트웍형 구조의 문서를 말하는 것으로, 월드 와이드 웹이 처음 개발되었을 때에는 텍스트 브라우저(text browser) 기반에서 운용되어 큰 호응을 얻지 못했으나 1993년 미국의 NCSA(National Center for Supercomputer Applications)에서의 모자이크 브라우저(mosaic browser)의 개발로 인해 문자, 영상, 동영상, 음성 정보 등을 포함하는GUI(Graphic User Interface) 환경 하에서 구동되기 시작하여 전세계적으로 큰 호응을 얻었다.

이러한 웹 브라우저(Web Browser)는 TV 방송으로 보자면 TV 수상기와 같다. 사용자 입장에서는 웹 브라우저만 익히면 당장 월드 와이드 웹을 이용할 수 있게 되는 것이다. 월드 와이드 웹의 복잡한 내부 작업은 웹 브라우저가 알아서 처리하므로, 사용자는 리모콘을 다루듯이 웹 브라우저를 조작하기만 하면 된다.

발명이 이루고자하는 기술적 과제

그러나 이러한 인터넷은 사용자가 원하는 홈 페이지에 접속하기 위해서는 해당 홈 페이지의 URL(Uniform Resource Locator)을 Cello, Lynx, Mosaic, Netscape, Explorer 등의 웹 브라우저에서 직접 치거나 검색엔진을 이용하고, URL의 구성은 자원이 저장된 상대방 컴퓨터의 주소 즉, http//www.A.co.kr 또는 http//www.A.com 또는 http//www.A.net 등으로 이루어져 있기 때문에 사용자가 접속하고자 하는 개인 또는 기업의 홈 페이지 주소가 A.co.kr이나 이를 정확히 인식하지 못해 http//www.A.com이나 http//www.A.net로 접속하는 경우가 발생하며, 또한 정확한 홈 페이지의 진위 여부를 파악하지 못하므로, 이를 사이버 범죄의 목적으로 하여 기업 또는 개인의 홈 페이지와 동일하게 홈 페이지를 꾸며 개인 신상 정보의 유출 또는 금전적 손해가 발생되는 문제점이 있었다.

본 발명의 목적은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로, 사용자가 접속을 원하는 홈 페이지 즉, 서버인지를 확인이 가능하도록 함으로써 사이버 범죄를 사전에 예방할 수 있는 전자인증에 의한 홈 페이지 검증방법을 제공하는데 있다.

발명의 구성 및 작용

상기와 같은 목적을 달성하기 위한 본 발명의 특징은,

웹 페이지 인증 프로그램에서 정적 문서를 소정의 암호화 과정을 거쳐 전자 서명하여 생성된 정적 서명된 문서를 저장하는 정적 문서 서명 단계와,

웹 브라우저에서 웹 페이지 인증 서버로 홈페이지에 대한 인증 요청을 하면 상기 웹 페이지 인증 서버는 임의의 포트를 사용하여 상기 웹 서버에게 홈 페이지를 요청하고, 상기 웹 서버는 웹 문서를 호출하여 상기 정적 서명된 문서를 웹 페이지 인증 서버로 전송하고, 웹 서버 응용 프로그램을 호출하여 동적 문서를 생성하여 생성된 상기 동적 문서를 상기 웹 페이지 인증 서버로 전송하는 문서 전송 단계와,

상기 웹 페이지 인증 서버는 전송된 문서가 상기 동적 문서이면 이를 상기 소정의 암호화 과정을 거쳐 전자 서명하여 생성된 동적 서명된 문서를 상기 웹 브라우저로 전송하고, 전송된 문서가 상기 정적 서명된 문서이면 이를 상기 웹 브라우저로 전송하는 동적 문서 서명 단계와,

상기 웹 브라우저로 상기 정적 서명된 문서 또는 동적 서명된 문서가 전송되면 이들을 웹 페이지 인증 클라이언트로 전송하고, 상기 웹 페이지 인증 클라이언트는 상기 정적 서명된 문서 또는 상기 동적 서명된 문서를 소정의 복호화 과정을 거쳐 전송된 상기 정적 문서 또는 동적 문서의 전자 서명이 정당하면 상기 정적 문서 또는 동적 문서를 상기 웹 브라우저로 전송하고, 전자 서명이 정당하지 않으면 문서의 변조를 알리는 경고를 디스플레이하는 전송 단계로 이루어지는 것을 특징으로 한다.

여기에서 상기 암호화 과정은,

상기 정적 문서 또는 동적 문서를 일방향 해쉬함수 알고리즘으로 메시지 다이제스트를 생성하는 단계와,

생성된 상기 메시지 다이제스트를 개인키로 전자 서명을 수행하는 단계와,

상기 정적 문서 또는 동적 문서와 전자 서명을 결합하여 상기 정적 서명된 문서 또는 동적 서명된 문서를 생성하는 단계로 이루어진다.

여기에서 또 상기 소정의 복호화 과정은,

상기 정적 서명된 문서 또는 동적 서명된 문서중 전자 서명을 추출하는 단계와,

추출된 전자 서명을 공개키로 복호화하여 상기 메시지 다이제스트를 획득하는 단계와,

상기 정적 서명된 문서 또는 동적 서명된 문서중 전자 서명을 제거하여 원본 정적 문서 또는 원본 동적 문서를 생성하는 단계와,

생성된 상기 원본 정적 문서 또는 원본 동적 문서를 상기 일방향 해쉬함수 알고리즘을 사용하여 비교용 메시지 다이제스트를 생성하는 단계와,

상기 메시지 다이제스트와 상기 비교용 메시지 다이제스트를 비교하여 서명이 정당한지의 여부를 확인하는 단계로 이루어진다.

여기에서 또 상기 임의의 포트는 상기 웹 서버와 상기 웹 페이지 인증 서버가 사용하는 통신 포트이다.

이하, 본 발명에 의한 전자인증에 의한 홈 페이지 검증방법의 구성 및 작용을 도 1 내지 도 2c를 참조하여 상세하게 설명하기로 한다.

도 1은 본 발명에 따른 전자인증에 의한 홈 페이지 검증방법의 개념을 설명하기 위한 개념도이다.

도 1을 참조하면, 본 발명에 따른 전자인증에 의한 홈 페이지 검증방법을 처리하기 위한 시스템은 웹 브라우저(100)와, 웹 페이지 인증 클라이언트(200)와, 웹 페이지 인증 서버(300)와, 웹 서버(400)와, 웹 페이지 인증 프로그램(500)과, 웹 서버 응용 프로그램(600)와, 웹 문서(700)로 구성된다.

웹 브라우저(100)는 동적 문서 또는 정적 문서를 디스플레이하고, 웹 페이지 인증 서버(300)로 홈 페이지에 대한 인증 요청을 수행하며, 정적 서명된 문서와 동적 서명된 문서를 웹 페이지 인증 클라이언트(200)로 전송한다.

웹 페이지 인증 클라이언트(200)는 웹 브라우저(100)의 호출에 따라 정적 서명된 문서 또는 동적 서명된 문서를 복호화 과정을 거쳐 비교용 메시지 다이제스트를 생성하고, 비교용 메시지 다이제스트와 메시지 다이제스트를 비교하여 동일하면 웹 브라우저(100)를 통해 사용자에게 디스플레이한다. 반대로 비교용 메시지 다이제스트와 메시지 다이제스트를 비교하여 동일하지 않으면 문서의 변조를 웹 브라우저(100)에게 알려 변제 메시지가 디스플레이되도록 한다.

웹 페이지 인증 서버(300)는 정적 서명된 문서에 한해서는 곧바로 웹 브라우저(100)로 전송하고, 동적 문서에 대해서는 암호화 과정을 통해 전자 서명을 수행하여 동적 서명된 문서를 생성한 후 이를 웹 브라우저(100)로 전송한다.

웹 서버(400)는 웹 브라우저(100)에게 홈 페이지에 대한 데이터를 전송하고, 특히 정적 문서에 대해서는 정적 서명된 문서를 전송하고, 웹 서버 응용 프로그램(600)에서 생성된 동적 문서는 생성후 곧바로 전송한다.

웹 페이지 인증 프로그램(500)은 HTML, TEXT등과 같은 정적 문서에 대하여 전자 서명하여 정적 서명된 문서를 저장한다.

웹 서버 응용 프로그램(600)은 웹 서버(400)의 호출에 의해 동적 문서를 생성하여 웹 서버(400)로 전송한다.

웹 문서(700)는 웹 서버(400)의 호출에 의해 정적 서명된 문서를 전송한다.

이하 본 발명에 의한 전자인증에 의한 홈 페이지 검증방법의 도 2a 내지 도 2c를 참조하여 상세하게 설명하면 다음과 같다.

도 2a 내지 도 2c는 본 발명에 따른 전자인증에 의한 홈 페이지 검증방법을 설명하기 위한 동작 흐름도이다.

먼저 웹 페이지 인증 프로그램(500)은 정적 문서를 일방향 해쉬함수 알고리즘으로 해쉬하여 메시지 다이제스트를 생성하고(S110), 생성된 메시지 다이제스트를 웹 페이지 인증 서버(300)의 개인키를 사용하여 전자서명한 후(S120), 정적 문서와 전자 서명을 결합해서 정적 서명된 문서를 생성하고(S130), 정적 서명된 문서를 웹 문서에 저장한다(S140).

이러한 상태에서 웹 브라우저(100)가 웹 페이지 인증 서버(300)에 인증된 홈 페이지를 요청하면(S210), 웹 페이지 인증 서버(300)는 웹 서버(400)에 홈 페이지를 요청한다.

웹 서버(400)는 정적 서명된 문서를 웹 페이지 인증 서버(300)로 전송하고(S220), 웹 페이지 인증 서버(300)는, 웹 서버 응용 프로그램(600)을 호출하여 이에서 동적 문서가 생성되도록 한후 이를 웹 서버(400)로 전송한다(S230).

그러면 웹 서버(400)는 전송된 동적 문서를 웹 페이지 인증 서버(300)로 전송하고(S240), 웹 페이지 인증 서버(300)는 전송된 문서가 동적 문서인지를 확인하여 동적 문서이면(S310), 이를 일방향 해쉬함수 알고리즘으로 해쉬하여 메시지 다이제스트를 생성한다(S320).

그런 다음 생성된 메시지 다이제스트를 웹 페이지 인증 서버(300)의 개인키로 전자 서명하고(S330). 동적 문서와 전자 서명을 결합하여 동적 서명된 문서를 생성하여(S340). 웹 브라우저(100)로 동적 서명된 문서를 기 설정된 포트(80번 포트)를 사용하여 전송한다(S350). 여기에서 웹 페이지 인증 서버(300)는 전송된 문서가 동적 문서가 아니면, 즉 정적 서명된 문서이면 그대로 웹 브라우저(100)로 기 설정된 포트를 사용하여 전송한다(S360).

정적 서명된 문서 또는 동적 서명된 문서 또는 이들을 전송받은 웹 브라우저(100)는 웹 페이지 인증 클라이언트(200)를 호출한다(S410).

호출된 웹 페이지 인증 클라이언트(200)는 정적 또는 동적 서명된 문서중 전자 서명을 추출하고(S420). 추출된 전자 서명을 웹 페이지 인증 서버(300)의 공개키로 복호화하여 메시지 다이제스트를 획득한다(S430).

그런 후 웹 페이지 인증 클라이언트(200)는 정적 또는 동적 서명된 문서중 전자 서명을 제거하여 원본 문서를 생성하고(S440). 원본 문서를 일방향 해쉬 알고리즘으로 비교용 메시지 다이제스트를 생성한다(S450).

또한 웹 페이지 인증 클라이언트(200)는 비교용 메시지 다이제스트와 메시지 다이제스트를 비교하여(S460). 동일하면 원본 문서를 웹 브라우저(100)로 전송한다(S470, S480). 반대로 비교용 메시지 다이제스트와 메시지 다이제스트가 서로 동일하지 않으면 원본 문서를 전송하지 않고 변조 메시지를 디스플레이한다(S490).

따라서 홈 페이지에서 제공되는 정적 및 동적 문서에 대한 인증을 웹 페이지 인증 서버를 통해 수행함으로써 클라이언트측에서는 정적 및 동적 문서의 진위 여부를 확인할 수 있다.

발명의 효과

이상에서 설명한 바와 같이 본 발명에 의한 전자인증에 의한 홈 페이지 검증방법에 의하면 웹 브라우저의 요청에 따라 웹 서버에서 생성되는 정적 또는 동적 문서의 진위 여부를 파악하여 사용자에게 알려 신뢰할 수 있는 인터넷 환경을 구축할 수 있도록 함으로써 사이버 범죄를 효과적으로 예방할 수 있다.

(57) 청구의 범위

청구항 1

웹 페이지 인증 프로그램에서 정적 문서를 소정의 암호화 과정을 거쳐 전자 서명하여 생성된 정적 서명된 문서를 저장하는 정적 문서 서명 단계와,

웹 브라우저에서 웹 페이지 인증 서버로 홈페이지에 대한 인증 요청을 하면 상기 웹 페이지 인증 서버는 임의의 포트를 사용하여 상기 웹 서버에게 홈 페이지를 요청하고, 상기 웹 서버는 웹 문서를 호출하여 상기 정적 서명된 문서를 웹 페이지 인증 서버로 전송하고, 웹 서버 응용 프로그램을 호출하여 동적 문서를 생성하여 생성된 상기 동적 문서를 상기 웹 페이지 인증 서버로 전송하는 문서 전송 단계와,

상기 웹 페이지 인증 서버는 전송된 문서가 상기 동적 문서이면 이를 상기 소정의 암호화 과정을 거쳐 전자 서명하여 생성된 동적 서명된 문서를 상기 웹 브라우저로 전송하고, 전송된 문서가 상기 정적 서명된 문서이면 이를 상기 웹 브라우저로 전송하는 동적 문서 서명 단계와,

상기 웹 브라우저로 상기 정적 서명된 문서 또는 동적 서명된 문서가 전송되면 이들을 웹 페이지 인증 클라이언트로 전송하고, 상기 웹 페이지 인증 클라이언트는 상기 정적 서명된 문서 또는 상기 동적 서명된 문서를 소정의 복호화 과정을 거쳐 전송된 상기 정적 문서 또는 동적 문서의 전자 서명이 정당하면 상기 정적 문서 또는 동적 문서를 상기 웹 브라우저로 전송하고, 전자 서명이 정당하지 않으면 문서의 변조를 알리는 경고를 디스플레이하는 전송 단계로 이루어지는 것을 특징으로 하는 전자인증에 의한 홈 페이지 검증방법.

청구항 2

제 1 항에 있어서,

상기 암호화 과정은,

상기 정적 문서 또는 동적 문서를 일방향 해쉬함수 알고리즘으로 메시지 다이제스트를 생성하는 단계와,

생성된 상기 메시지 다이제스트를 개인키로 전자 서명을 수행하는 단계와,

상기 정적 문서 또는 동적 문서와 전자 서명을 결합하여 상기 정적 서명된 문서 또는 동적 서명된 문서를 생성하는 단계로 이루어지는 것을 특징으로 하는 전자인증에 의한 홈 페이지 검증방법.

청구항 3

제 1 항에 있어서,

상기 소정의 복호화 과정은,

상기 정적 서명된 문서 또는 동적 서명된 문서중 전자 서명을 추출하는 단계와,

추출된 전자 서명을 공개키로 복호화하여 상기 메시지 다이제스트를 획득하는 단계와,

상기 정적 서명된 문서 또는 동적 서명된 문서중 전자 서명을 제거하여 원본 정적 문서 또는 원본 동적 문서를 생성하는 단계와,

생성된 상기 원본 정적 문서 또는 원본 동적 문서를 상기 일방향 해쉬함수 알고리즘을 사용하여 비교용 메시지 다이제스트를 생성하는 단계와,

상기 메시지 다이제스트와 상기 비교용 메시지 다이제스트를 비교하여 서명이 정당한지의 여부를 확인하는 단계로 이루어지는 것을 특징으로 하는 전자인증에 의한 홈 페이지 검증방법.

청구항 4

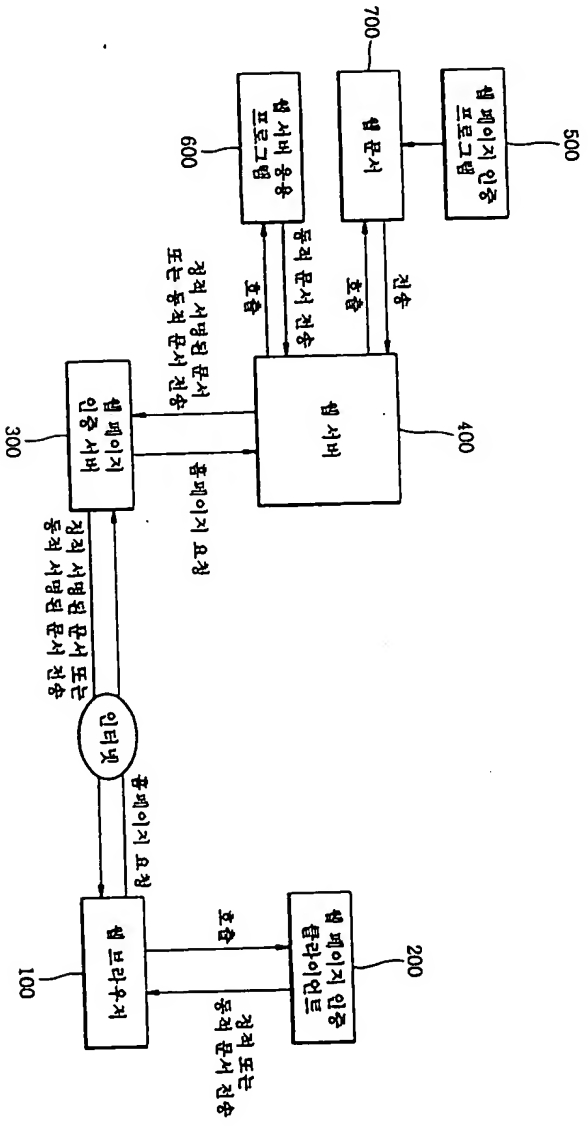
제 1 항에 있어서,

상기 임의의 포트는,

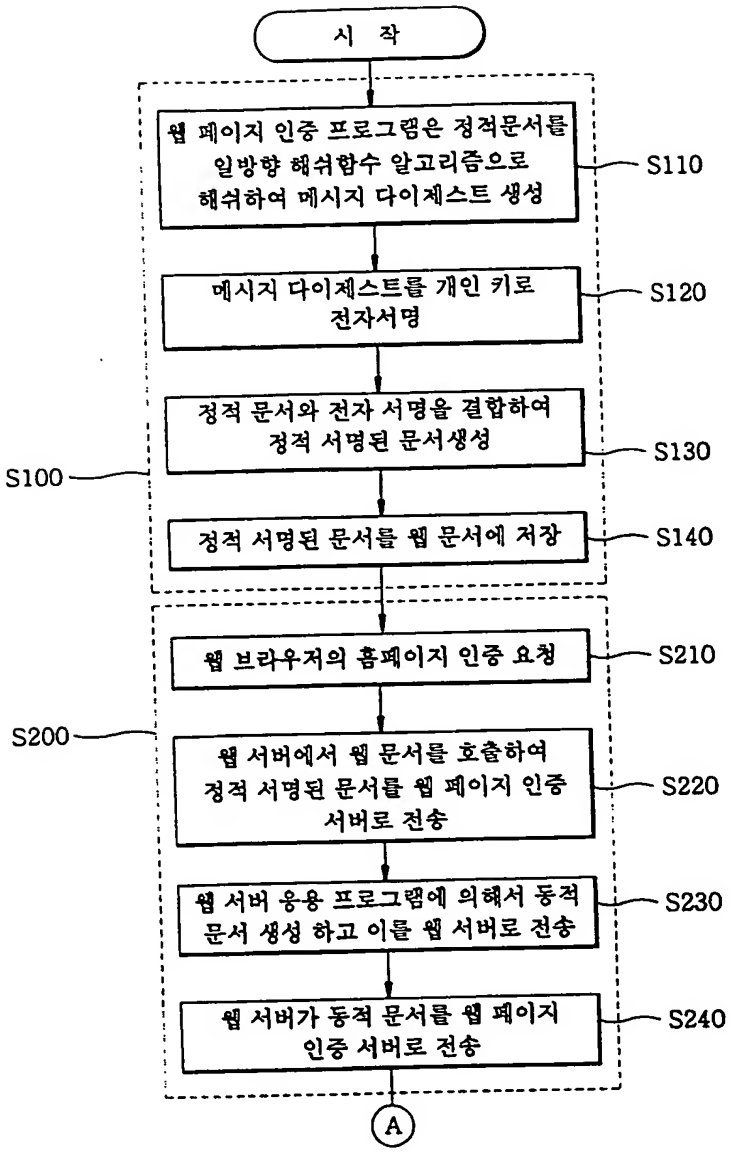
상기 웹 서버와 상기 웹 페이지 인증 서버가 사용하는 통신 포트임을 특징으로 하는 전자 인증에 의한 홈페이지 검증 방법.

도면

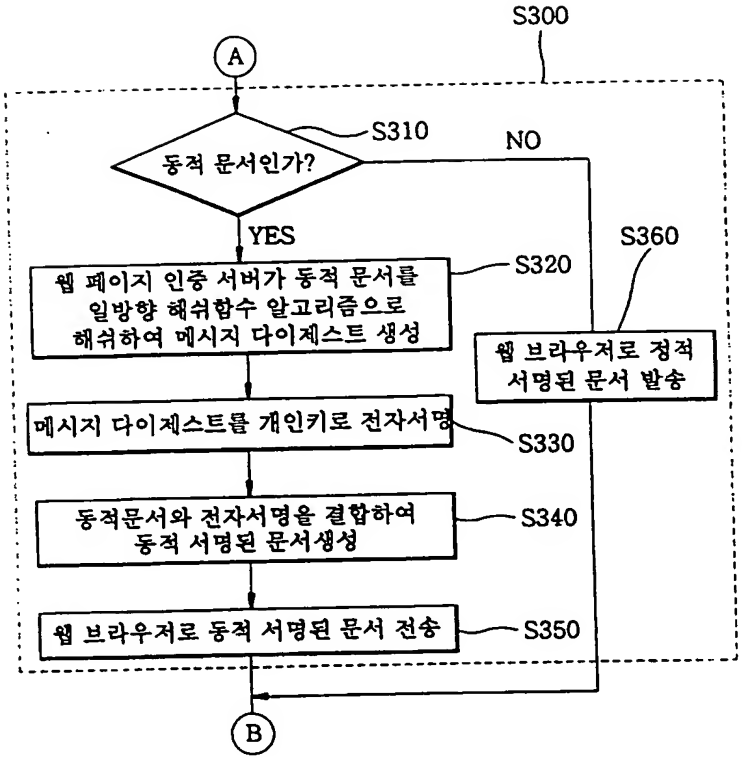
도면1



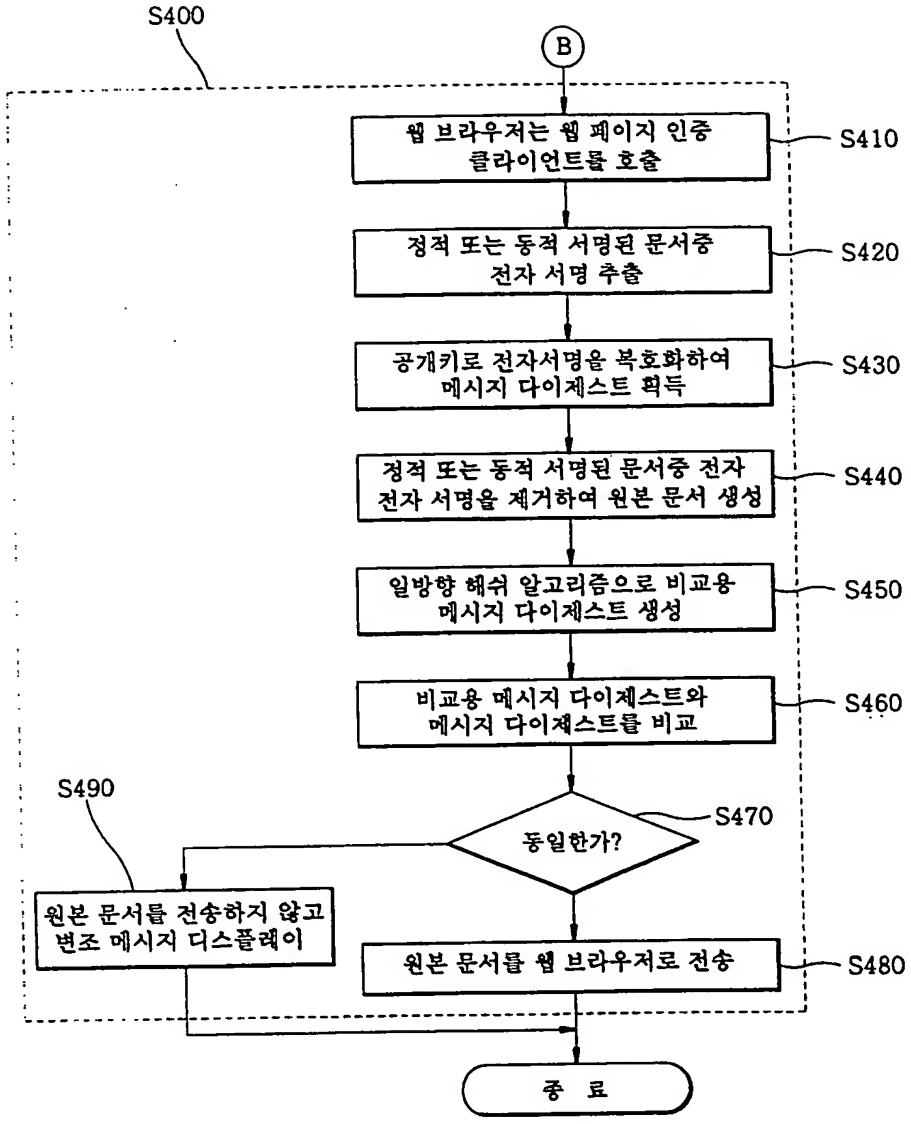
도면2a


시 작
웹 페이지 인증 프로그램은 정적문서를 일방향 해쉬함수 알고리즘으로 해쉬하여 메시지 다이제스트 생성
S110
메시지 다이제스트를 개인 키로 전자서명
S120
정적 문서와 전자 서명을 결합하여 정적 서명된 문서생성
S130
S100
정적 서명된 문서를 웹 문서에 저장
S140
웹 브라우저의 홈페이지 인증 요청
S210
S200
웹 서버에서 웹 문서를 호출하여 정적 서명된 문서를 웹 페이지 인증 서버로 전송
S220
웹 서버 응용 프로그램에 의해서 동적 문서 생성 하고 이를 웹 서버로 전송
S230
웹 서버가 동적 문서를 웹 페이지 인증 서버로 전송
S240
A

도면2b


S300
A
S310
동적 문서인가?
NO
YES
S360
웹 페이지 인증 서버가 동적 문서를 일방향 해쉬함수 알고리즘으로 해쉬하여 메시지 다이제스트 생성
S320
웹 브라우저로 정적 서명된 문서 발송
메시지 다이제스트를 개인키로 전자서명
S330
동적문서와 전자서명을 결합하여 동적 서명된 문서생성
S340
웹 브라우저로 동적 서명된 문서 전송
S350
B

도면2c


S400
B
웹 브라우저는 웹 페이지 인증 클라이언트를 호출
S410
정적 또는 동적 서명된 문서중 전자 서명 추출
S420
공개키로 전자서명을 복호화하여 메시지 다이제스트 획득
S430
정적 또는 동적 서명된 문서중 전자 전자 서명을 제거하여 원본 문서 생성
S440
일방향 해쉬 알고리즘으로 비교용 메시지 다이제스트 생성
S450
비교용 메시지 다이제스트와 메시지 다이제스트를 비교
S460
동일한가?
S470
S490
원본 문서를 전송하지 않고 변조 메시지 디스플레이
원본 문서를 웹 브라우저로 전송
S480
종 료

T.SJ488

(19) 大韓民国特許庁(KR)
(12) 公開特許公報(A)

(51) Int.Cl.[7]
G06F 17/00

(11) 公開番号：特2000-0036707
(43) 公開日付：2000.07.05.

(21) 出願番号：10-2000-0015429
(22) 出願日付：2000.03.27

(71) 出願人：株式会社ドリームシキュリティ ユン グム
(72) 発明者：キム デ シク

審査請求：有り

(54) 電子認証によるホームページの検証方法

要約

本発明はウェブサーバで静的文書と動的文書をウェブブラウザに転送時、静的文書は事前にウェブページ認証プログラムで暗号化過程を経て電子署名した静的署名された文書を生成してディレクトリーに格納した状態でウェブブラウザでホームページに対する認証要請をすると、ウェブサーバでウェブページ認証サーバに静的署名された文書を転送し、ウェブサーバ応用プログラムによって生成された動的文書はウェブページ認証サーバで暗号化過程を経て電子署名した動的署名された文書を生成し、動的または静的署名された文書をウェブブラウザに転送し、ウェブブラウザに静的または動的署名された文書が転送されるとウェブブラウザはウェブページ認証クライアントを呼び出してウェブページの認証クライアントから所定の復号化過程を経て転送された静的文書または動的文書の電子署名が正当であるどうかを把握して、署名が正当であれば、静的文書または動的文書をウェブブラウザに転送することを特徴とする。

従って、上記のようになされた本発明によると、ウェブブラウザの要請に応じてウェブページ認証サーバで生成される静的または動的文書の真偽の如何を把握して使用者に知らせることによって信頼できるインターネット環境を構築できる。

(57) 請求の範囲

請求項 1

ウェブページ認証プログラムで静的文書を所定の暗号化過程を経て電子署名して生成された静的署名された文書を格納する静的文書署名段階と、

ウェブブラウザでウェブページ認証サーバにホームページに対する認証要請をすると上記ウェブページ認証サーバは任意のポートを使用して上記ウェブサーバにホームページを要請し、上記ウェブサーバはウェブ文書を呼び出して上記静的署名された文書をウェブページ認証サーバに転送し、ウェブサーバ応用プログラムを呼び出して動的文書を生成して生成された上記動的文書を上記ウェブページ認証サーバに転送する文書転送段階と、

上記ウェブページ認証サーバは転送された文書が上記動的文書であれば、これを上記所定の暗号化過程を経て電子署名して生成された動的署名された文書を上記ウェブブラウザに転送し、転送された文書が上記静的署名された文書であれば、これを上記ウェブブラウザに転送する動的文書署名段階と、

上記ウェブブラウザに上記静的署名された文書または動的署名された文書が転送されると、これらをウェブページ認証クライアントに転送し、上記ウェブページ認証クライアントは上記静的署名された文書または上記動的署名された文書を所定の復号化過程を経て転送された上記静的文書または動的文書の電子署名が正当であれば、上記静的文書または動的文書を上記ウェブブラウザに転送し、電子署名が正当でなければ文書の変造を知らせる警告をディスプレイする転送段階とからなることを特徴とする電子認証によるホームページ検証方法。

請求項 2

第 1 項において、

上記暗号化過程は、

上記静的文書または動的文書を一方向ハッシュ関数アルゴリズムでメッセージダイジェストを生成する段階と、

生成された上記メッセージダイジェストを個人キーで電子署名を行う段階と、

上記静的文書または動的文書と電子署名とを結合して上記静的署名された文書または動的署名された文書を生成する段階とからなることを特徴とする電子認証によるホームページ検証方法。

請求項3

第1項において、

上記所定の復号化過程は、

上記静的署名された文書または動的署名された文書のうち電子署名を抽出する段階と、

抽出された電子署名を公開キーで復号化して上記メッセージダイジェストを獲得する段階と、

上記静的署名された文書または動的署名された文書のうち電子署名を除去して原本静的文書または原本動的文書を生成する段階と、

生成された上記原本静的文書または原本動的文書を上記一方向ハッシュ関数アルゴリズムを使用して比較用メッセージダイジェストを生成する段階と、

上記メッセージダイジェストと上記比較用メッセージダイジェストとを比較して署名が正当であるかどうかを確認する段階とからなることを特徴とする電子認証によるホームページ検証方法。

請求項4

第1項において、

上記任意のポートは、

上記ウェブサーバと上記ウェブページ認証サーバが使用する通信ポートであることを特徴とする電子認証によるホームページ検証方法。